WM-4T1i Module Installation and User Guide

Extreme Networks, Inc.
3585 Monroe Street
Santa Clara, California 95051
(888) 257-3000
http://www.extremenetworks.com

Published: June 2001
Part number: 100095-00 Rev. 01

Contents

Preface

1 Installing the WM-4T1i Module

2 Configuring the T1 Physical Link

3 Configuring PPP and MLPPP

Index

Index of Commands

Preface

This Preface provides an overview of this guide, describes guide conventions, and lists other publications that may be useful.

Introduction

This guide provides the required information to install the WM-4T1i module in an Alpine 3800 series switch from Extreme Networks and perform the initial module configuration tasks.

This guide is intended for use by network administrators who are responsible for installing and setting up network equipment. It assumes a basic working knowledge of:

- Local area networks (LANs).
- Ethernet concepts.
- Ethernet switching and bridging concepts.
- Routing concepts.
- Internet Protocol (IP) concepts.
- Routing Information Protocol (RIP) and Open Shortest Path First (OSPF).
- Simple Network Management Protocol (SNMP).

If the information in the release notes shipped with your module differs from the information in this guide, follow the release notes.

Conventions

Table 1 and Table 2 list conventions that are used throughout this guide.

Table 1: Notice Icons

Icon	Notice Type	Alerts you to...
ⓘ	Note	Important features or instructions.
⚠	Caution	Risk of personal injury, system damage, or loss of data.
⚡	Warning	Risk of severe personal injury.

Table 2: Text Conventions

Convention	Description
`Screen displays`	This typeface indicates command syntax, or represents information as it appears on the screen.
`Screen displays bold`	This typeface indicates how you would type a particular command.
The words “enter” and “type”	When you see the word “enter” in this guide, you must type something, and then press the Return or Enter key. Do not press the Return or Enter key when an instruction simply says “type.”
[Key] names	Key names are written with brackets, such as [Return] or [Esc]. If you must press two or more keys simultaneously, the key names are linked with a plus sign (+). Example: Press [Ctrl]+[Alt]+[Del].
Words in *italicized* type	Italics emphasize a point or denote new terms at the place where they are defined in the text.

Related Publications

The publications related to this one are:

- ExtremeWare™ release notes
- *ExtremeWare Software User Guide*
- *Alpine 3800 Series Switch Hardware Installation Guide*
- *Alpine Module Installation Note*

Documentation for Extreme Networks products is available on the World Wide Web at the following location:

http://www.extremenetworks.com/

1 Installing the WM-4T1i Module

This chapter covers the following topics:

- Installing the WM-4T1i Module on page 1-2
- Ports and Connectors on page 1-3
- WM-4T1i Module LEDs on page 1-3
- Installing the WM-4T1i Module Software on page 1-5

Overview

The Extreme Networks WM-4T1i module is an four-port T1 module that can be configured to use Multilink PPP to aggregate Ethernet traffic across multiple T1 physical links. The module has two 10/100 Mbps Ethernet ports.

The WM-4T1i module also has six internal loopback ports. The Alpine 3800 switch modules have hardware queues associated with the output of each port for QoS (rate shaping and priority queueing). To implement ingress QoS, you needed to use the hardware queues associated with a second port as a loopback port for ingress QoS

Installing the WM-4T1i Module

All Alpine ™ 3800 series switch module cards (SMMi modules and I/O modules) are hot-swappable. You do not need to power off the system to remove or insert a module card.

Caution: Service to Alpine modules should be performed by trained service personnel only. Before installing or removing any components of the system, or before carrying out any maintenance procedures, read the safety information provided in Appendix A of the Alpine Hardware Installation Guide.

Warning: You must install blank panels in empty slots to ensure adequate system cooling.

To remove and replace a module card, follow these steps:

1 Prior to removing/installing a module card into the Alpine 3804 or Alpine 3808 chassis, put on the ESD wrist strap that is provided with the chassis, and connect the metal end to the ground receptacle located on the top-right corner of the Alpine front panel.

2 Loosen the module card by unscrewing the screws using a #2 Phillips-head screwdriver.

3 Rotate the ejector/injector handles to disengage the module card from the backplane.

Note: Blank panels do not have ejector/injector handles, because they do not engage the backplane. They are secured entirely by the retaining screws. In addition, the retaining screws are not captive.

4 Slide the module card out of the chassis.

5 Slide the new module card into the appropriate slot of the chassis (SMMi modules into the orange slot, I/O modules into Slots 1 through 4 on the Alpine 3804, or Slots 1 through 8 on the Alpine 3808), until it is fully seated in the backplane.

Caution: Ensure that the sheet metal of the module, and not the PCB board, engages the card cage runners.

As the module begins to seat in the chassis, the ejector/injector handles will begin to close.

6 To secure the module in the chassis, close the ejector/injector handles by pushing them toward the center of the module card, and tighten the screws using a #2 Phillips-head screwdriver.

Note: Tighten the screws before inserting additional modules. If you insert additional modules before tightening the screws, you might unseat modules that you have not secured.

Caution: You can only install I/O modules in the slots labeled Slot 1 through Slot 4 on the Alpine 3804, or Slot 1 through Slot 8 on the Alpine 3808. Forceful insertion can damage the I/O module and the connector pins on the backplane.

Ports and Connectors

The WM-4T1i module is show in Figure 1-1.

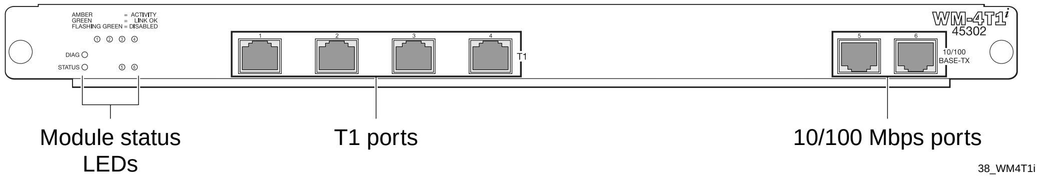

Figure 1-1: WM-4T1i Module

The WM-4T1i module has four T1 ports and two 10/100 Ethernet ports. The WM-4T1i also has six internal loopback ports. Internal loopback ports allow you to configure bi-directional rate-limiting without tying up any of the external ports for ingress rate shaping. Internal loopback ports are marked with the notation “iL” when displayed on the command line or with ExtremeWare Vista Web access.

WM-4T1i Module LEDs

The WM-4T1i module LEDs are shown in Figure 1-1.

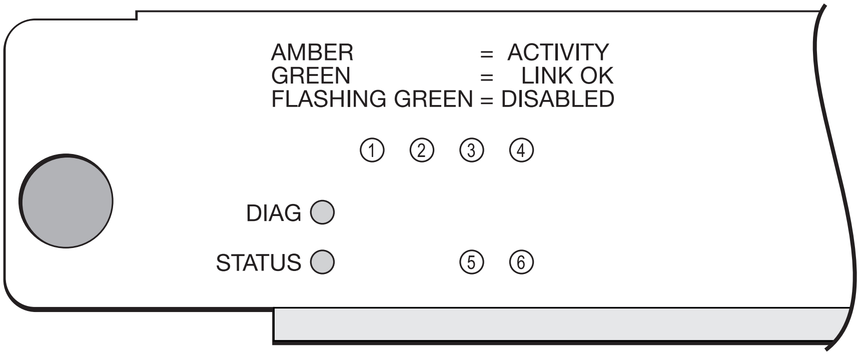

Figure 1-2: WM-4T1i LEDs

Table 1-1 describes the LED behavior on the WM-4T1i module.

Table 1-1: WM-4T1i Module LEDs

LED	Color	Indicates
Status	Off	No power
	Amber	Module seated in chassis
	Green	Module powered up
Diag	Green (blinking)	Power-on Self Test (POST) is running
	Off	Normal operation
T1 port (1-4)	Amber	Near-end fault detected (for example, no cable)
	Rapidly blinking amber	Far-end fault detected
	Slowly blinking amber	Physical link present, but no higher-layer link (port misconfigured or disabled)
	Green	Physical link present, higher-layer link established, no traffic
	Alternating green and amber	Physical link present, higher-layer link established, traffic present
	Green (blinking)	Loopback testing mode
10/100 port (5,6)	Off	No link present
	Green	Link present
	Alternating green and amber	Traffic present

The slowly blinking LEDs cycle once per second. The rapidly blinking LEDs cycle twice a second.

Installing the WM-4T1i Module Software

Once the WM-4T1i module is installed in the chassis, you must download an image file to the module.

The image file contains the executable code that runs on the module. As new versions of the image are released, you should upgrade the software running on your module.

The image is downloaded from either a Trivial File Transfer Protocol (TFTP) server on the network or from a PC connected to the serial port using the XMODEM protocol. Downloading a new image involves the following steps:

- Load the new image onto a TFTP server on your network (if you will be using TFTP).
- Load a new image onto a PC (if you will be using XMODEM).
- Download the new image to the module using the command

  ```
  download image slot <slot> [<ipaddress> | <hostname>] <filename>
  {primary | secondary}
  ```

  where the following is true:

  `slot` — Is the slot in which the WM-4T1i module is installed.

  `ipaddress` — Is the IP address of the TFTP server.

  `hostname` — Is the hostname of the TFTP server. (You must enable DNS to use this option. See the *ExtremeWare Software User Guide* for more information.)

  `filename` — Is the filename of the new image.

  `primary` — Indicates the primary image.

  `secondary` — Indicates the secondary image.

The module can store up to two images; a primary and a secondary. When you download a new image, you must select into which image space (primary or secondary) the new image should be placed. If not indicated, the primary image space is used.

You can select which image the switch will load on the next reboot by using the following command:

```
use image [primary | secondary]
```

2 Configuring the T1 Physical Link

This chapter covers the following topics:

- Configuring T1 Physical link on page 2-1
- Monitoring T1 Physical Link on page 2-6

Overview

T1 is a mature technology originally developed for voice telephone transmission. It was used to aggregate a number of voice lines into a single connection to the telephone network. Today T1 is also widely used to transmit digital data using widely available equipment and established wiring commonly available in diverse locations.

Configuring T1 Physical link

There are a number of parameters that can be configured for a T1 link. If you have control of both sides of the link, then the default configuration is probably the best choice. If you must connect to a line controlled by another organization, you will need to configure the line to correspond with the settings at the other end. You can specify the following parameters:

- Alarms
- Cable length

- Clock Source
- Facility Data Link
- Framing
- Inband Loopback Detection
- Linecoding
- Yellow Alarms

Alarms

The T1 standard, ANSI T1.403, Bellcore TR-54016 and others, defines red, yellow, and blue alarms.

A red alarm occurs when the T1 signal is lost or an out of frame error occurs. An out of frame error can be caused when the framing type configured for the local interface does not match the framing type of the incoming T1 signal or when the incoming signal does not contain a T1 framing pattern.

A yellow alarm is also called a Remote Alarm Indication (RAI). When the remote end of a link does not receive a signal, it will transmit a yellow alarm signal back to the local end.

A blue alarm is also called an Alarm Indication Signal (AIS). A blue alarm indicates that a device somewhere upstream has experienced a loss of signal.

The default value is on. To configure whether alarms are generated and detected, use the following command:

```
config ports <portlist> t1 alarms [on | off]
```

Yellow alarms can be configured when T1 alarms are enabled. See “Yellow Alarms” on page 2-5 for more details on the following command:

```
config ports <portlist> t1 yellow [detection | generation | both | off]
```

Cable length

Longer cable lengths cause greater loss for the T1 signal, so the transmitter hardware must transmit at a higher level to transmit data successfully. However, too high a signal level can cause crosstalk from one cable to another. The `config ports t1` `cablelength` command allows you to control the transmitter signal level for your conditions. Typically, your service provider will suggest the correct level.

For short haul connections (less then 700 feet) the typical equipment uses less sensitive receivers. The transmitter level is usually set by selecting a cable length in feet, from the following values: 133, 266, 399, 533 or 655. Choose the next higher value if your cable length does not match one of the values. For example, choose 133 for a 50 foot cable and 533 for a 450 foot cable. The default value is 133, which corresponds to cables in the range of 0-133 feet.

For longer distances (up to 6000 feet) the typical equipment uses more sensitive receivers, and crosstalk is more likely to occur. Under these conditions, the transmitter level is set by selecting a transmitter attenuation level in dB from the following values: -22.5, -15, -7.5, or 0.

From lowest to highest transmitter level, use the following values for the `config port t1 cablelength` command: -22.5 db, -15 db, -7.5 db, 0 db, 133 feet, 266 feet, 399 feet, 533 feet, and 655 feet.

To configure the cable length, use one of the following commands:

```
config ports <portlist> t1 cablelength [0 | -7.5 | -15 | -22.5] db
config ports <portlist> t1 cablelength [133 | 266 | 399 | 533 | 655]
feet
```

CLOCK SOURCE

A clock is used to synchronize data transmission on the line. Generally, one end of the T1 link provides the master clock, and the other end of the link recovers the clock from the signal on the line. By default the clock source is derived from the line. If needed, an internal clock is available. To configure the clock source, use the following command:

```
config ports <portlist> t1 clocksource [internal | line]
```

Note: If the clock source is configured as “line”, but the clock cannot be recovered from the signal on the line, the hardware will use the internal clock instead.

Facility Data Link

Facility data link (FDL) uses twelve bits in the ESF frame to signal information about line and connection status. Since FDL is only meaningful for ESF framing, FDL settings are ignored when a port is configured for SF framing. See “Framing” for information on configuring framing.

The two standards supported for FDL are ATT, described by the ATT 54016 specification, and ANSI, described by the T1.403 standard. The default value is off. To configure FDL, use the following command:

```
config ports <portlist> t1 fdl [off | att | ansi]
```

Framing

Framing is used to synchronize data transmission on the T1 line. Framing allows the hardware to determine when each packet starts and ends. The two choices for framing are Super Frame (SF), also known as D4, and Extended Super Frame (ESF). The ESF scheme is a newer standard and is enabled by default. To choose the framing scheme, use the following command:

```
config ports <portlist> t1 framing [esf | sf]
```

If you choose to use SF framing, you should disable yellow alarm detection for the T1 line. SF framing may generate false yellow alarms. See “Yellow Alarms” on page 2-5 for more details.

Inband Loopback Detection

When inband loopback detection is enabled, a specific sequence of data in the signal payload from the remote end of the T1 link will cause the local end to enter network line loopback mode and send any received signal back to the remote end. Inband loopback detection is only possible if the FDL standard is configured as ATT. See “Facility Data Link” on page 2-3 for more details. By default, inband loopback detection is off. See “Loopback” on page 2-6 for more information about loopback modes. To configure inband loopback detection, use the following command:

```
config ports <portlist> t1 lbdetect [off | inband]
```

Linecoding

Linecoding is the convention used to encode signals for transmission over the T1 line. You can choose from two linecoding standards, bipolar eight zero suppression (B8ZS) or alternate mark inversion (AMI). The default value is B8ZS. To configure linecoding, use the following command:

```
config ports <portlist> t1 linecoding [b8zs | ami]
```

Yellow Alarms

A yellow alarm occurs on a device when its signal is not received at the remote end. It is also called a Remote Alarm Indication (RAI). You can disable detection and generation of yellow alarms for a T1 port. When SF framing is used, yellow alarm detection and generation should be set to off, because detection of yellow alarms is not reliable when data traffic is transmitted with SF framing (data traffic often contains bit combinations that do not occur for encoded voice traffic). The default value for yellow alarm generation and detection is both. To configure yellow alarms, use the following command:

```
config ports <portlist> t1 yellow [detection | generation | both | off]
```

T1 Port Configuration Commands

Table 2-1 describes the commands used to configure a T1 port.

Table 2-1: T1 Port Configuration Commands

Command	Description
config ports <portlist> t1 alarms [on | off]	Enables and disables alarms. The default setting is on.
config ports <portlist> t1 cablelength [[133 | 266 | 399 | 533 | 655] feet | [0 | -7.5 | -15 | -22.5] dB]	Specifies the cablelength attached to the T1 port. The default is 0 dB.
config ports <portlist> t1 clock source [internal | line]	Specifies the clock source used for transmission. The default setting is line.
config ports <portlist> t1 fdl [off | att | ansi]	Specifies the facilities data link (FDL) format for the port. You cannot use FDL with SF framing.
config ports <portlist> t1 framing [esf | sf]	Specifies the framing type. The default setting is esf, Extended Super Frame (ESF). If sf is chosen, Super Frame (SF), set yellow alarm detection to off, since a yellow alarm can be incorrectly detected with SF framing.
config ports <portlist> t1 lbdetect [off | inband]	Enables and disables the port to respond to loopback requests from the remote end. The default setting is off.
config ports <portlist> t1 linecode [b8zs | ami]	Sets the linecoding. The default setting is b8zs.
config ports <portlist> t1 yellow [detection | generation | both | off]	Enable and disable yellow alarm detection and generation.

Monitoring T1 Physical Link

T1 devices have a built-in facility designed for troubleshooting the physical link, called loopback. The T1 link can also be monitored using show commands to display the current configuration of the link, any alarms on the link, link statistics, and link errors.

Loopback

The T1 device can be set up to loopback, that is, return a transmitted signal back to the sender so it can be compared with the original. There are several different types of loopback available to test different parts of the device and the line, specified in the T1 standards.

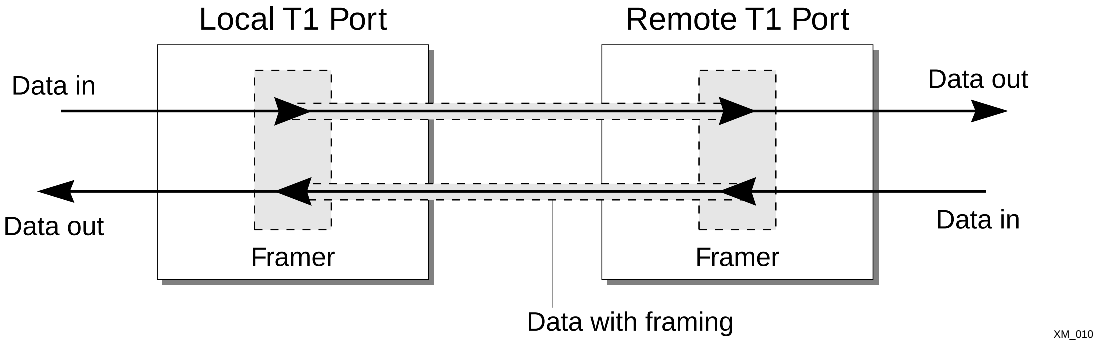

Figure 2-1: Normal operation of T1 link

During normal operation of a T1 link, as the local data stream enters the framer, the appropriate framing bits are inserted into the data, and the framed signal is transmitted to the remote end. At the remote end, the process is reversed as the framing bits are discarded and the data stream is passed to the remote system.

Loopback can be enabled on the near-end or the far-end of the link. The near-end loopback modes are controlled directly by the hardware on the near-end. Far-end loopback modes require the cooperation of the far-end hardware. A message is sent to the far-end to cause it to enter a far-end loopback mode. When loopback is enabled on a T1 port, the green port LED will blink.

Near-end Loopback Modes

The near-end of the link can be enabled for the following three loopback modes:

- Local
- Network Line
- Network Payload

The local loopback mode reflects the data stream internally to the near-end. The network line loopback mode reflects the signal to the far-end. The network payload mode reflects the data carried in the signal and regenerates framing information back to the far-end.

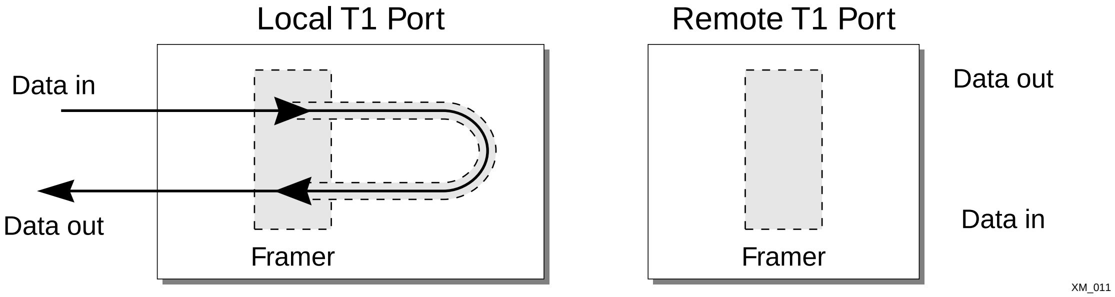

Figure 2-2: Local loopback mode

Local Loopback Mode. When the local port is enabled for local loopback, the local data stream goes into the framer and the framing bits are inserted into the data, but the data is not transmitted to the remote end. Instead, it is sent back through the local framer, the framing bits are discarded, and the original data is returned. This mode tests the local end.

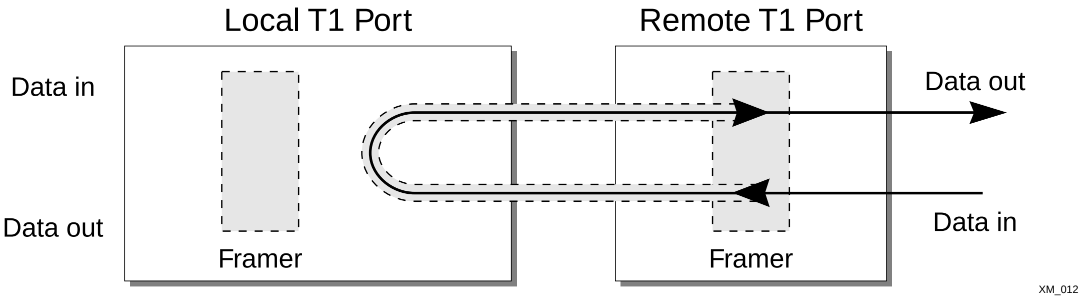

Figure 2-3: Network line loopback mode

Network Line Loopback Mode. When the local port is enabled for network line loopback mode, the received signal is sent back to the remote end without reframing the data. This mode primarily tests the integrity of the line from the remote side.

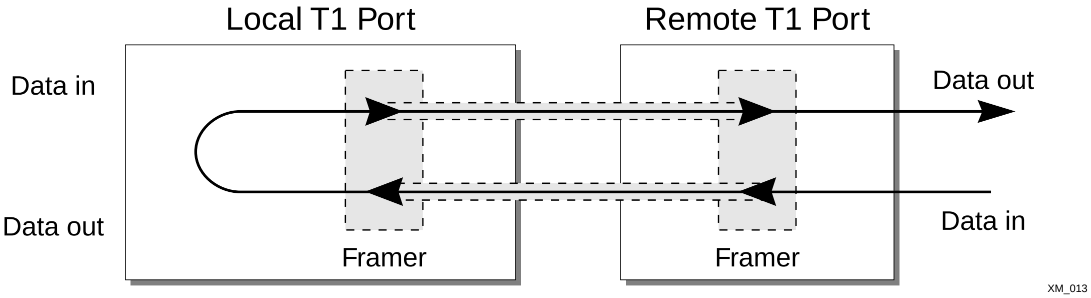

Figure 2-4: Network payload loopback mode

Network Payload Loopback Mode. When the local port is enabled for network payload mode, the framer removes the framing bits from the received signal and recovers the transmitted data. This same data is then reframed and transmitted back to the remote end. This mode tests the line and the local circuitry from the remote side.

Far-End Loopback Modes

The far-end of the link can be enabled for the following two loopback modes:

- Remote Line
- Remote Payload

The remote line mode reflects the received signal back to the near-end. The remote payload mode reflects the data and regenerates the framing information back to the near-end.

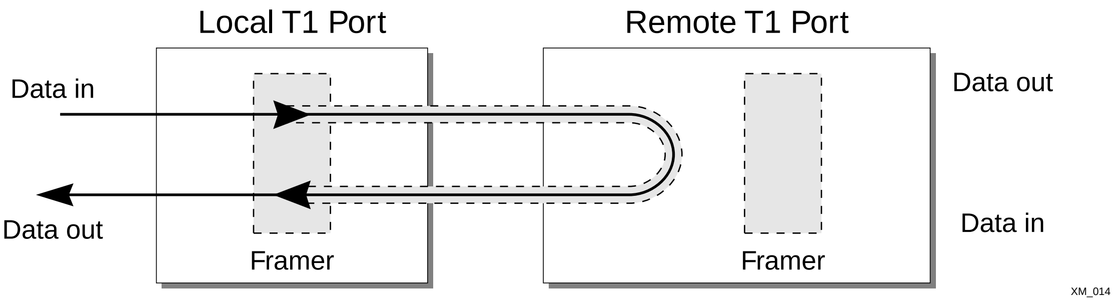

Figure 2-5: Remote line loopback mode

Remote Line Loopback Mode. When the local port is enabled for remote line loopback mode, it sends a request to the remote end to enter the equivalent of network line loopback mode. The signal transmitted to the remote end will be retransmitted as received back to the local end.

Note: If the line is configured to use the ATT FDL standard, the remote end must be configured to detect inband loopback requests for the remote end to enter remote line loopback mode.

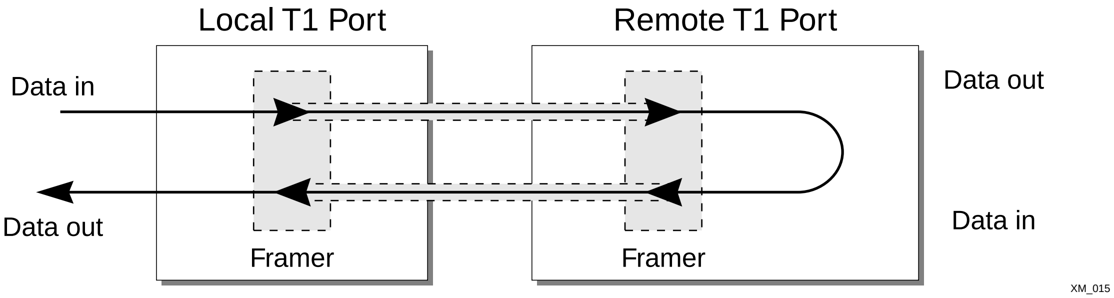

Figure 2-6: Remote payload loopback mode

Remote Payload Loopback Mode. When the local port is enabled for remote payload loopback mode, it sends a request to the remote end to enter the equivalent of network payload loopback mode. When the remote end enters loopback mode, the framer at the remote end removes the framing bits from the received signal and recovers the transmitted data. This same data is then reframed and transmitted back to the local end.

Enabling Loopback Mode

To enable a loopback mode, use one of the following commands:

```
enable ports <portlist> t1 loopback local
enable ports <portlist> t1 loopback network [line | payload]
enable ports <portlist> t1 loopback remote [line | payload]
```

Disabling Loopback Mode

Use the following command to return the near and remote side of a T1 loopback mode to normal mode:

```
disable ports <portlist> t1 loopback
```

You can also use the following command to return the remote port to normal function from loopback mode:

```
enable ports <portlist> t1 loopback remote loopdown
```

T1 Port Monitoring Commands

Table 2-2 describes the commands used to monitor a T1 port.

Table 2-2: T1 Port Monitoring Commands

Command	Description
disable ports <portlist> t1 loopback	Disable the current loopback mode and return to normal function.
enable ports <portlist> t1 loopback [local | network [line | payload] | remote [line | payload | loopdown]]	Enable the port to locally loopback, to cause the remote link to loopback, and to stop the loopback.
show ports {<portlist>} {t1} stats	Displays real-time port statistics.
show ports {<portlist>} t1 alarms	Displays real-time port alarms.
show ports {<portlist>} t1 configuration	Displays the port configuration and status.

Table 2-2: T1 Port Monitoring Commands (continued)

Command	Description
show ports {<portlist>} t1 errors [near-end | far-end] [totals | intervals | current]	Displays current and past errors.
show ports {<portlist>} t1 info	Displays the port configuration and status.

3 Configuring PPP and MLPPP

This chapter covers the following topics:

- Multilink PPP and Multilink Groups on page 3-2
- Configuring a PPP/MLPPP Link on page 3-3
- Monitoring PPP/MLPPP Links on page 3-6
- PPP/MLPPP Configuration Examples on page 3-6

Overview

Point-to-Point Protocol (PPP) is used across the entire range of communication speeds and devices found on the internet. Typically, PPP uses Layer 3 to connect two broadcast networks, say two ethernet LANs, into a single WAN by transporting IP packets over a link. PPP can also use Layer 2 to bridge packets from one VLAN to another.

Multilink PPP (MLPPP) is a protocol for combining a number of PPP links into one bundle that transports traffic over the links in the bundle. A multilink group is just a bundle of individual PPP links that are configured to work together as a single link. With a multilink group configured, it is easy to add or remove additional PPP links to provide bandwidth as needed. The multilink group balances traffic among the individual PPP links and properly sequences packets across the multilink group.

Typically, you would add a multilink group to a VLAN, configure the multilink group by adding T1 ports and configuring PPP/MLPPP parameters, and finally, enable the multilink group.

Multilink PPP and Multilink Groups

Each multilink PPP group is given a name, up to 16 characters in length. All named components of the switch configuration must have unique names, so multilink groups and VLANs cannot have identical names. See the *ExtremeWare Software User Guide* for more information on allowable names for named components. Components are named using the `create` command. Once a component is named, you do not need to use the keyword for the component (see the shortcut below).

Create the multilink group using the following command:

```
create multilink <groupname>
```

Once the multilink group is created, assign ports to it by using the following command:

```
config multilink <groupname> add ports <portlist>
```

or you can use the following shortcut:

```
config <groupname> add ports <portlist>
```

If the first port added to a multilink group is already configured for PPP, the multilink group will inherit the configuration of the first port. Any other ports added to the link will be configured to match the multilink configuration. The next section lists the configuration commands for multilink groups and single PPP links.

Once the multilink group has been configured, it is added to a VLAN so that it can pass traffic from the VLAN across the link. To add a multilink group to a VLAN, use the following command:

```
config vlan <vlan> add multilink <groupname>
```

Typically the last step in configuring a multilink group is to use the following command to enable it:

```
enable multilink <groupname>
```

Any changes to an enabled multilink group will not take effect until the the multilink group is restarted. To restart a multilkink group, use the following command:

```
restart multilink <groupname>
```

Configuring a PPP/MLPPP Link

All of the PPP configuration commands can be used to configure a single port or to configure a multilink group, so the following sections for PPP links also apply to MLPPP links. To configure a PPP / MLPPP link you will need to choose the authentication and encapsulation for the link.

If you change the configuration of an enabled PPP or MLPPP link, the changes will not take effect until the link is restarted. To restart a PPP link, use the following command:

```
restart ports <portlist>
```

To restart an MLPPP link, use the following command:

```
restart multilink <groupname>
```

Authentication

By default, no authentication is configured on PPP links since the WM-4T1i module will typically be used with leased lines—where both sides of the link are controlled and authentification is not required. If authentication is needed, the WM-4T1i module supports using PAP or CHAP. PPP authentication protocol (PAP) authenticates a user as the connection is established by sending a username and password. Challenge Handshake Authentication Protocol (CHAP) authenticates a user by sending a challenge across the link. The remote end calculates a response based on the user password and sends the response back across the link. CHAP is a more secure authentication protocol than PAP. The link can also be configured to attempt to use CHAP first, followed by PAP, if CHAP fails.

To configure authentication on a PPP link, use the following command:

```
config ppp authentication [off | chap | pap | chap-pap] [ports
<portlist> | multilink <groupname>]
```

PPP Link Username

When the local end of a link initiates a PPP connection, the local end must send the appropriate authentication information. For PAP it sends the username and password, for CHAP it sends the username and must respond correctly to the challenge, and for no authentication it sends nothing. To configure the username and password used to initiate the link, use the following command:

```
config ppp user <username> {encrypted} <password> [ports <portlist> |
multilink <groupname>]
```

The encrypted keyword is used to hide the password when the switch configuration is displayed, it does not control whether the password is encrypted across the link during authentication.

PPP User Accounts

When the remote end initiates the link, the local end must verify the authentication information. The local end maintains a list of authorized user accounts and passwords. To add a user to the list, use the following command:

```
create account pppuser <name> {encrypted} {<password>}
```

Encapsulation

The packets passed over the PPP link can use either bridged or routed encapsulation. You would use bridged packets if you plan to have VLANs span the PPP link. You would use routed packets if the link connects two different routed networks or separate VLANs.

Using bridged packets allows the VLAN tags to be carried across the PPP link. Bridged packets are transported using the PPP Bridging Control Protocol (BCP), described in RFC 2878. When the encapsulation is set to BCP, 802.1Q and 802.1p information is preserved and transported across the link. On a WM-4T1i module, a VLAN may only contain one BCP encapsulated link.

Routed packets are transported across a PPP/MLPPP link using IP Control Protocol (IPCP), described in RFC 1332. This is the encapsulation that is familiar to most users of PPP. The routed packets do not contain Ethernet headers so cannot preserve VLAN tags. The IP addresses used for the PPP/MLPPP link are taken from the IP address assigned to the VLAN at each end of the link. The VLAN that contains the IPCP encapsulated PPP/MLPPP ports cannot contain other ports. In other words, the only ports allowed in the VLAN are those that make up the IPCP encapsulated link.

You must have one and only one encapsulation type configured on a PPP/MLPPP link. Setting BCP encapsulation off implies that IPCP encapsulation is on. The default setting is BCP encapsulation on and IPCP encapsulation off. To configure encapsulation, use the following command:

```
config ppp [bcp [on | off] | ipcp [on | off]] [ports <portlist> |
multilink <groupname>]
```

PPP/MLPPP Configuration Commands

Table 3-1 describes the commands used to configure a PPP/MLPPP link.

Table 3-1: PPP/MLPPP Configuration Commands

Command	Description
config multilink <groupname> add ports <portlist>	Adds ports to a multilink group.
config multilink <groupname> delete ports <portlist>	Removes ports from a multilink group.
config ppp authentication [off | chap | pap | chap-pap] [ports <portlist> | multilink <groupname>]	Sets the authentication method for a PPP link or a MLPPP multilink group. The default setting is to use no authentication.
config ppp [bcp [on | off] | [ipcp [on | off]] [ports <portlist> | multilink <groupname>]	Sets the encapsulation method for a PPP/MLPPP link. You cannot set both to on, or both to off. Configuring bcp on implies ipcp off; configuring ipcp on implies bcp off. The default setting is bcp on.
config ppp user <username> {encrypted} <password> [ports <portlist> | multilink <groupname>]	Sets the username sent to the remote end of a PPP/MLPPP link for authentication.
config vlan <vlan> add multilink <groupname>	Adds an MLPPP multilink group to a VLAN.
config vlan <vlan> delete multilink <groupname>	Removes an MLPPP multilink group from a VLAN.
create account pppuser <name> {encrypted} {<password>}	Adds a username that will be accepted by the local end during authentication.
create multilink <groupname>	Creates a multilink group.
delete multilink <groupname>	Deletes a multilink group.
delete account pppuser <username>	Removes a username from the local authentication list.
disable multilink <groupname>	Disables a multilink group.
enable multilink <groupname>	Enables a multilink group (and enables all ports in the group).

Table 3-1: PPP/MLPPP Configuration Commands (continued)

Command	Description
restart multilink <groupname>	Restarts multilink group. Configuration changes made to an enable multilink group will not take effect until the group is restarted.
unconfig ppp port <portlist>	Resets the port to the default PPP configuration; no authentication and BCP encapsulation.

Monitoring PPP/MLPPP Links

The following commands monitor the status of the PPP and MLPPP links.

Table 3-2: PPP/MLPPP Show Commands

Command	Description
show multilink <groupname>	Displays the configuration of the multilink group.
show multilink [<groupname>] stats {detail}	Displays multlink group statistics.
show multilink [<groupname>] t1 alarms {detail}	Displays T1 alarm status for multilink groups.
show multilink [<groupname>] t1 errors [near-end | far-end] [totals | intervals | current]	Displays T1 error statistics for a multilink group.
show ppp {<portlist>} {detail}	Shows PPP configurations.
show accounts pppuser	Show the PPP accounts on the switch.

PPP/MLPPP Configuration Examples

The following examples show how to configure multilink groups.

Configuring a Bridged PPP/MLPPP Link Example

The following example shows how to configure a BCP-encapsulated multilink group. BCP is the default encapsulation, so it is not explicitly included in this example. The `config ports t1 clocksource` command is included to show where you might need to configure the T1 parameters for your link. Each T1 port in the multilink group will have the same T1 and PPP configurations. If you change the configuration for a single port, the change will affect the entire group.

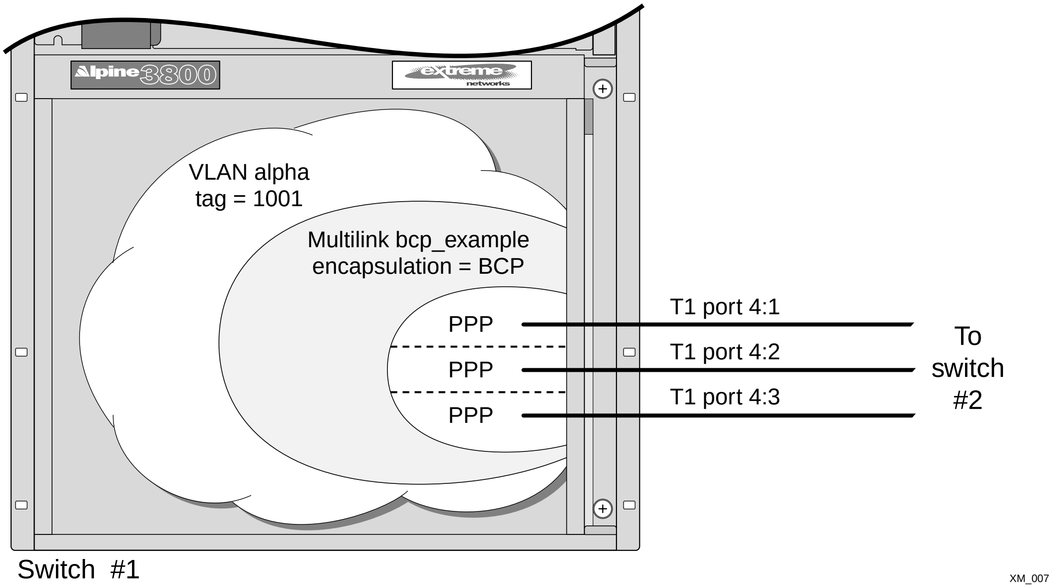

Figure 3-1: BCP multilink example

```
config default delete ports 4:1-4:3
create vlan alpha
config alpha tag 1001
create multilink bcp_example
config ports 4:1-4:3 t1 clocksource internal
config bcp_example add ports 4:1-4:3 tag
config alpha add multilink bcp_example
enable bcp_example
```

Configuring a Routed PPP/MLPPP Link Example

The following example shows how to configure a IPCP-encapsulated multilink group. The VLAN that contains the IPCP-encapsulated multilink group cannot contain any other ports.

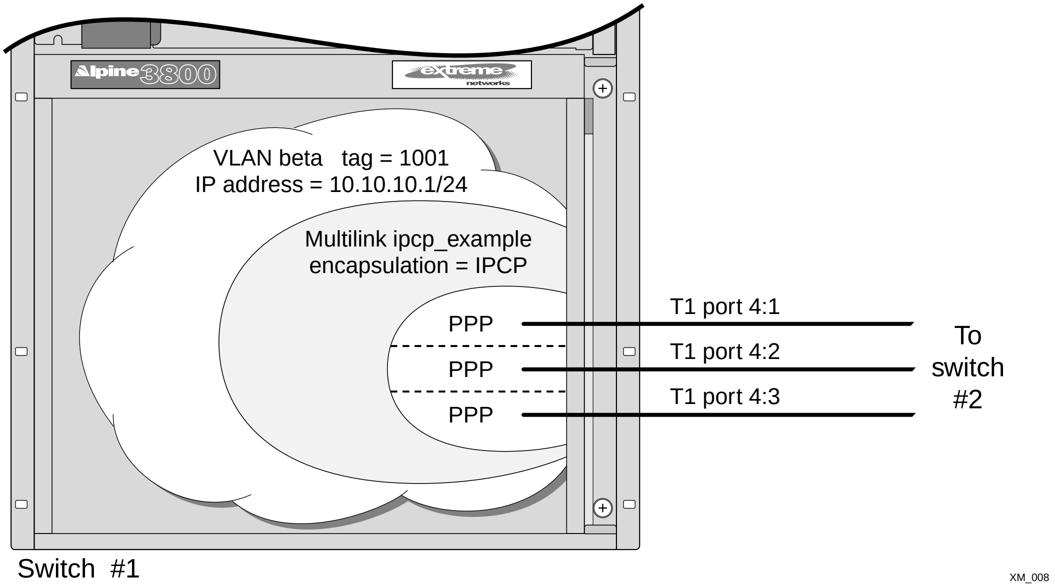

Figure 3-2: IPCP multilink example

```
config default delete ports 4:1-4:3
create vlan beta
config beta tag 1001
config beta ipaddress 10.10.10.1/24
create multilink ipcp_example
config ipcp_example add ports 4:1-4:3 tag
config ppp ipcp on ports 4:1-4:3
config beta add multilink ipcp_example
enable ipcp_example
```

Index

Index of Commands